Preserving Peer Replicas By Rate-Limited Sampled Voting

Petros Maniatis, Mema Roussopoulos, TJ Giuli,
David S. H. Rosenthal, Mary Baker, Yanto Muliadi
Stanford University

Peer to Peer Seminar

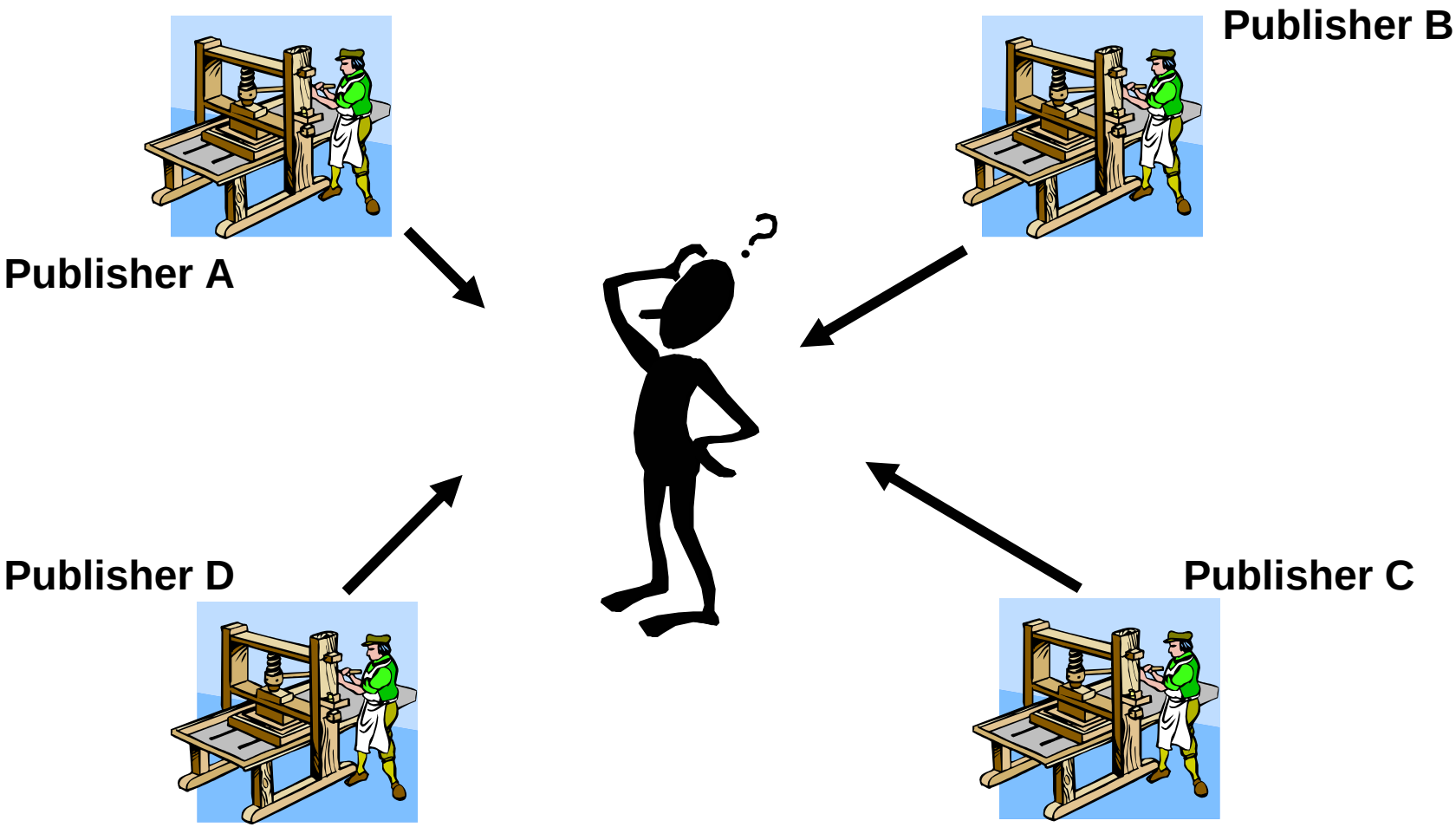
Prof. Dr.-Ing. Gerhard Weikum

Presentation by: **Renata Dividino**

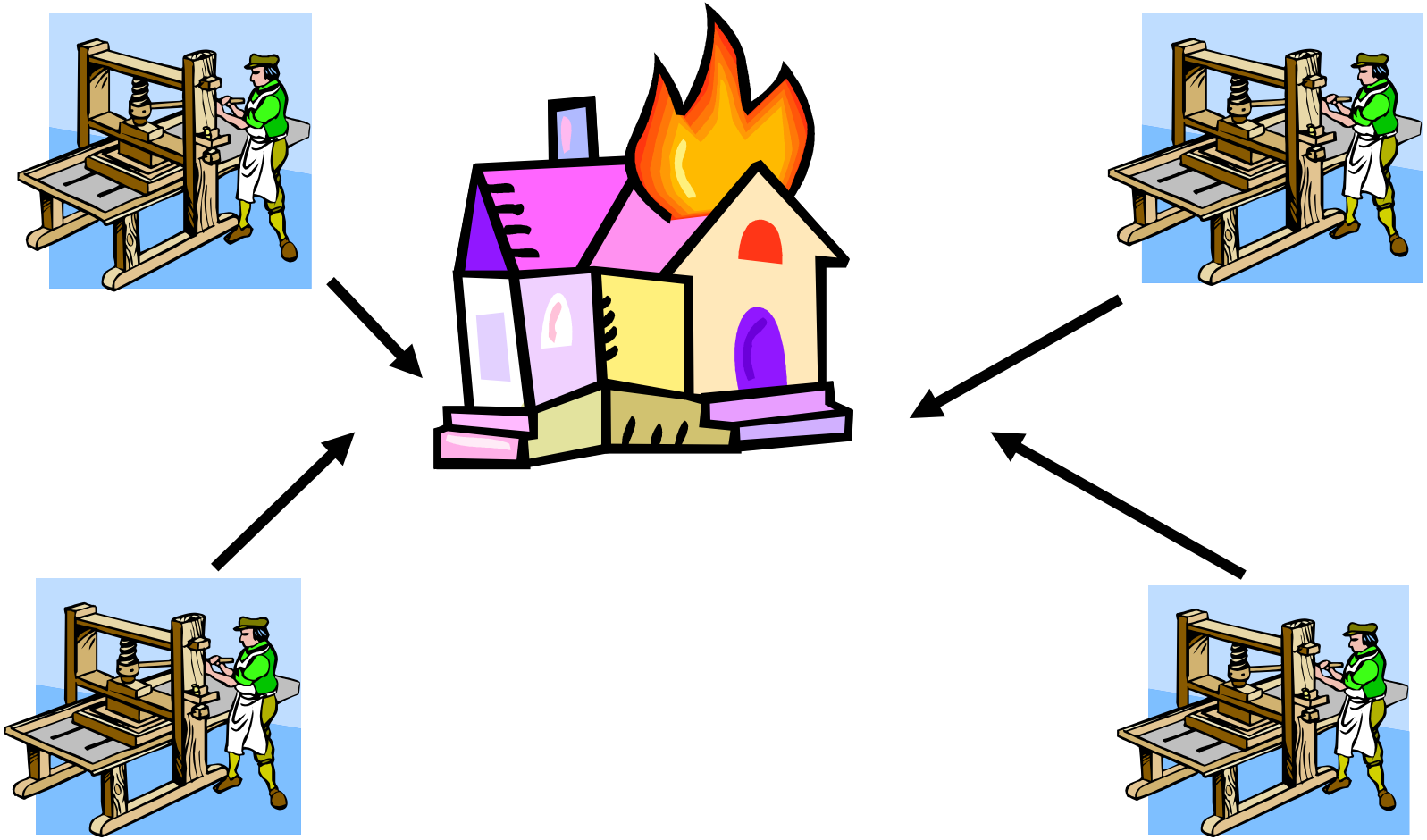
Overview

- Motivation
- Digital Preservation System
- Problems / Challenges
- What's LOCKSS ?
- Protocol Description
- Protocol Analysis
- Adversary
- Results
- Conclusion

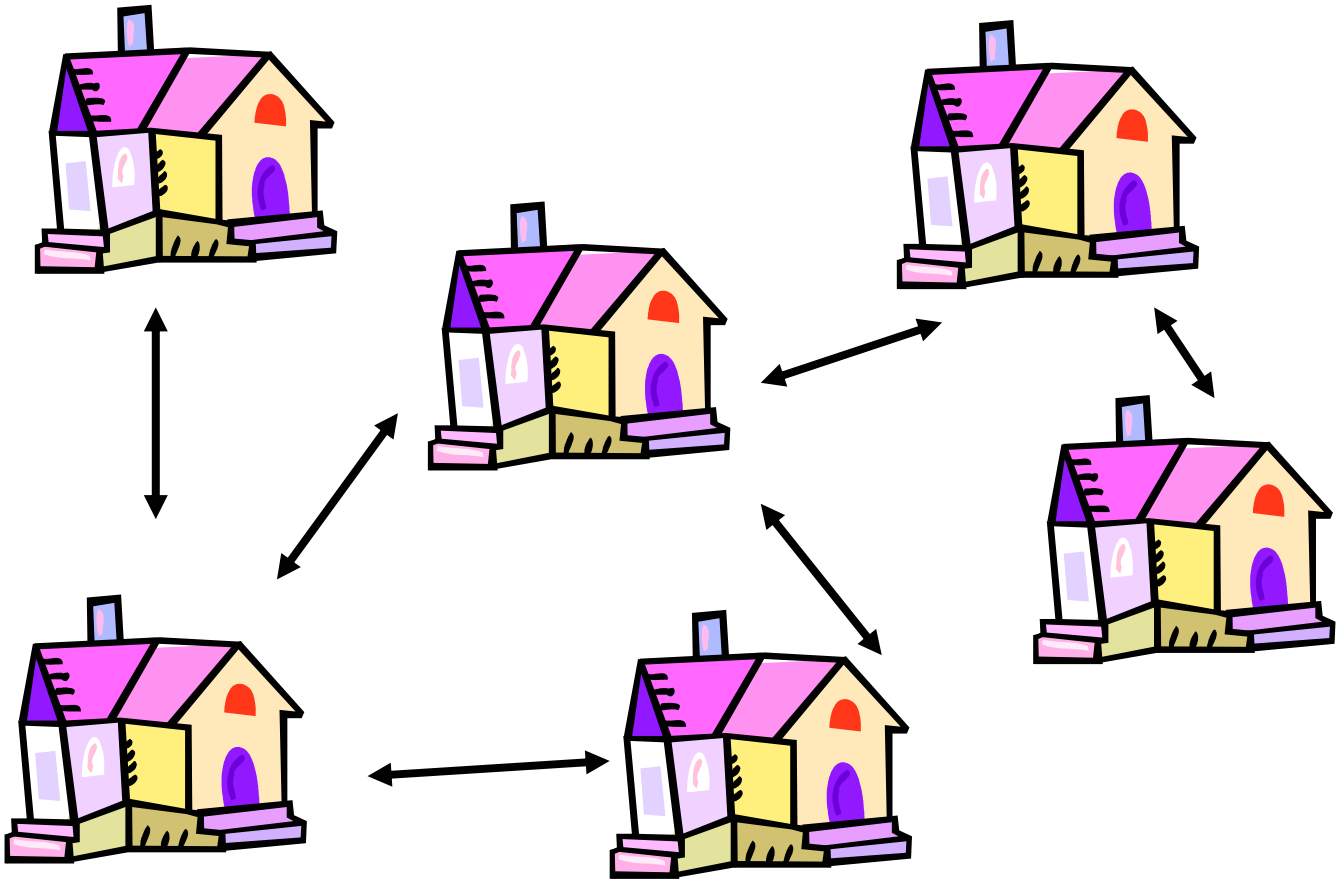
Motivation: Why Libraries?



Motivation:
Why Distributed Libraries?



Motivation: Distributed Digital Libraries



Digital Preservation System

- Collect material
- Distribute it to local readers
- Preserve by cooperating with others that hold the same material to detect and repair damage

Problems / Challenges

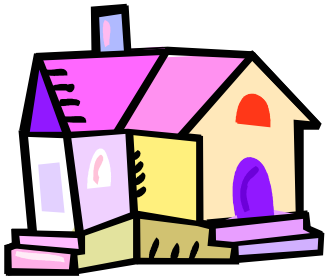
- Malign / Loyal Peers
- Sybil Effect

- Common Solution – Add extra effort involved in messages.

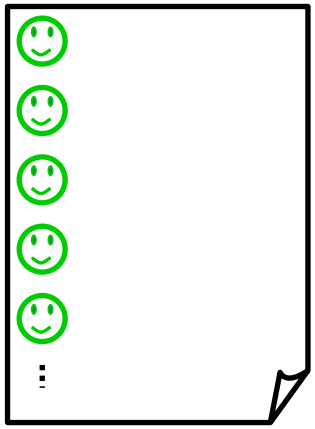
What´s LOCKSS ?

- The LOCKSS (Lots Of Copies Keep Stuff Safe)
  - large number of independent, low-cost, persistent web caches,
  - protocol,
  - detect and repair damage by voting in „opinion polls“ on their documents caches.

Protocol Description (1)

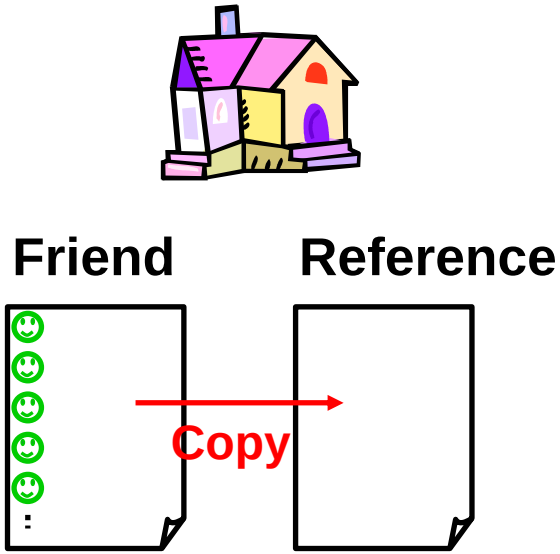


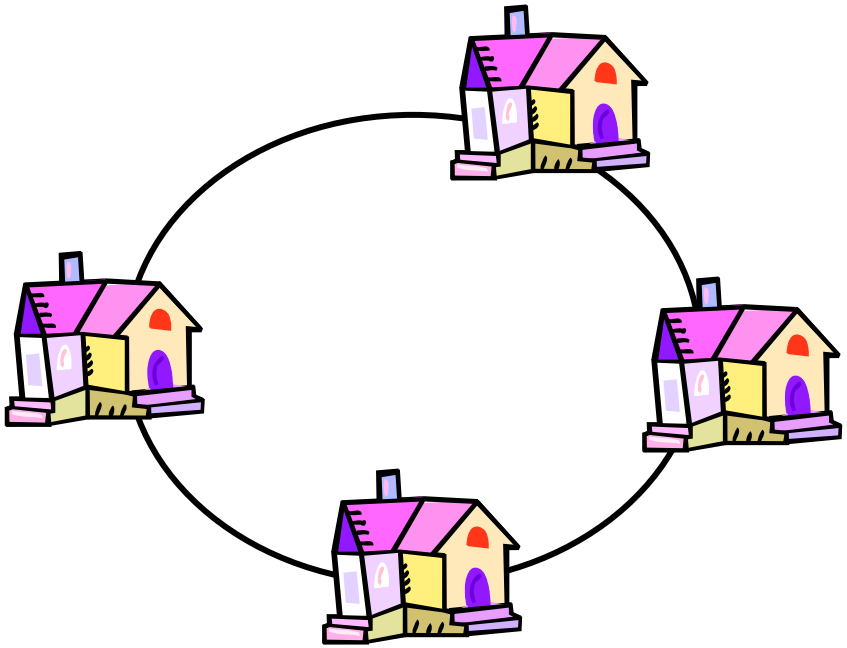
Friend List



For each document (or Archival Unit - AU) a library maintains a Friend List.

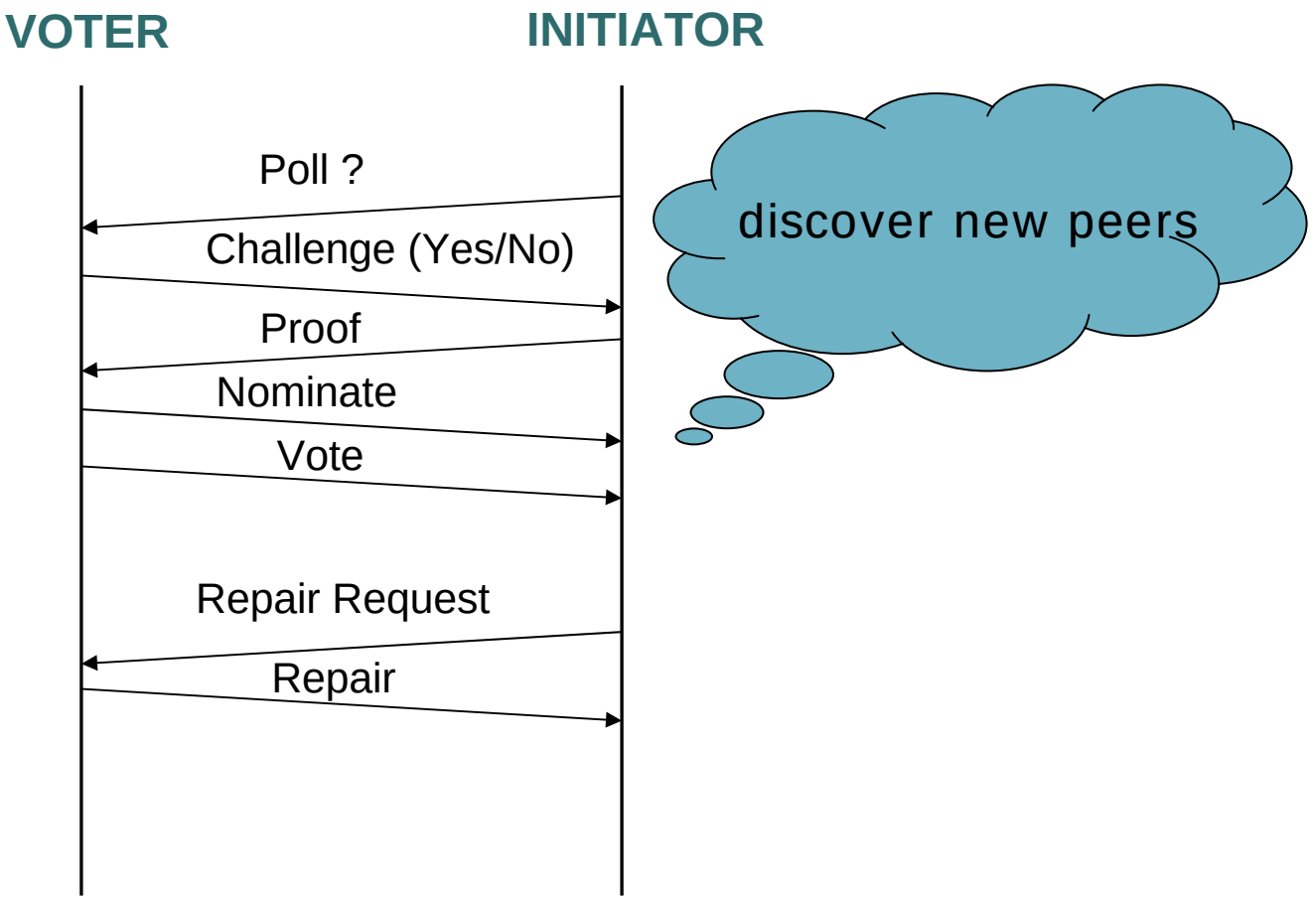
Protocol Description (2)



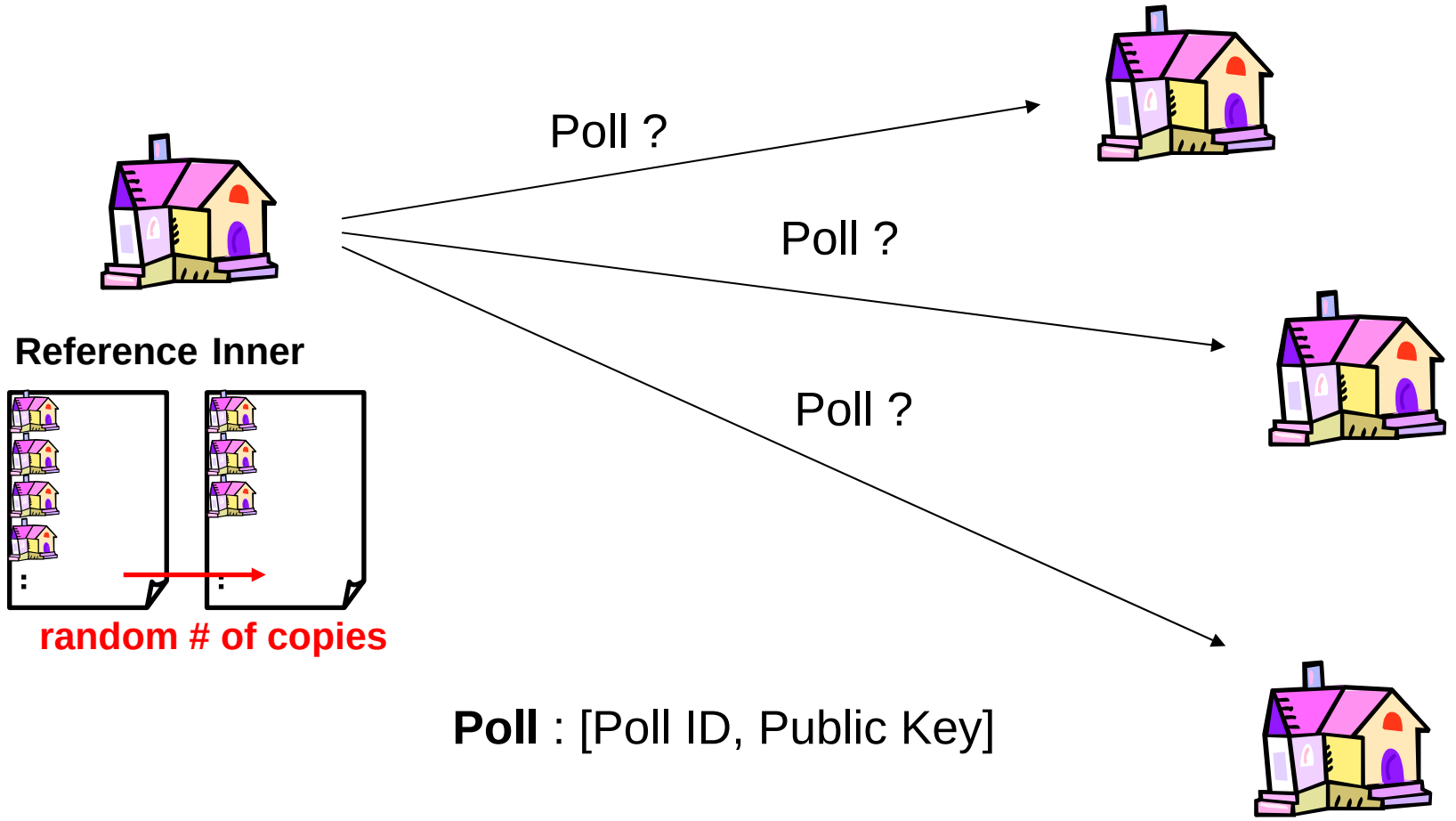


When a library joins a network,
it creates its **Reference List**

Protocol Description (3)

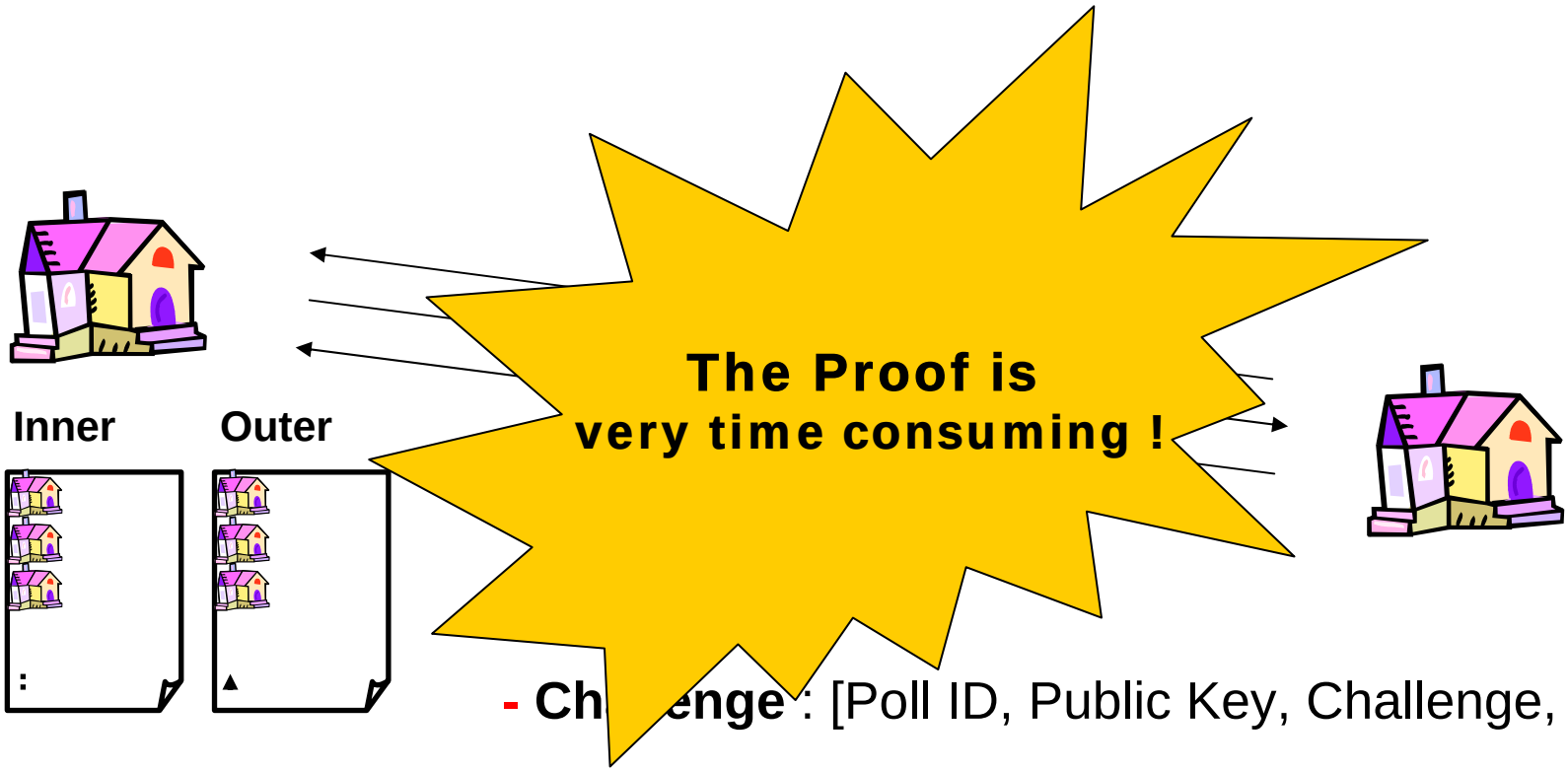


Protocol Description (4)



Poll : [Poll ID, Public Key]

Protocol Description (5)

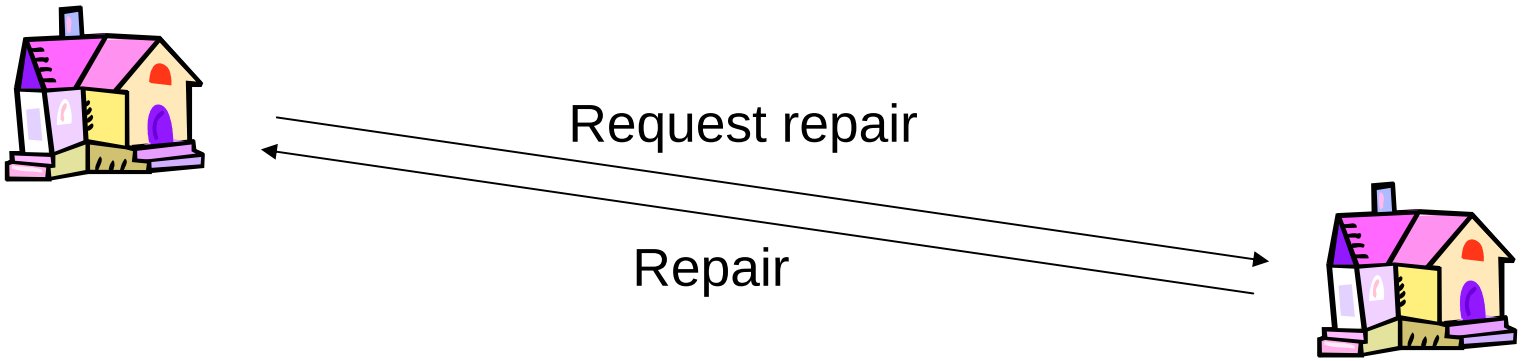


- **Challenge** : [Poll ID, Public Key, Challenge, Yes/No]
+ **Proof** : [Poll ID, poll Effort Proof]
- **Nominate** : [Poll ID, Nominations]

Protocol Description (6)

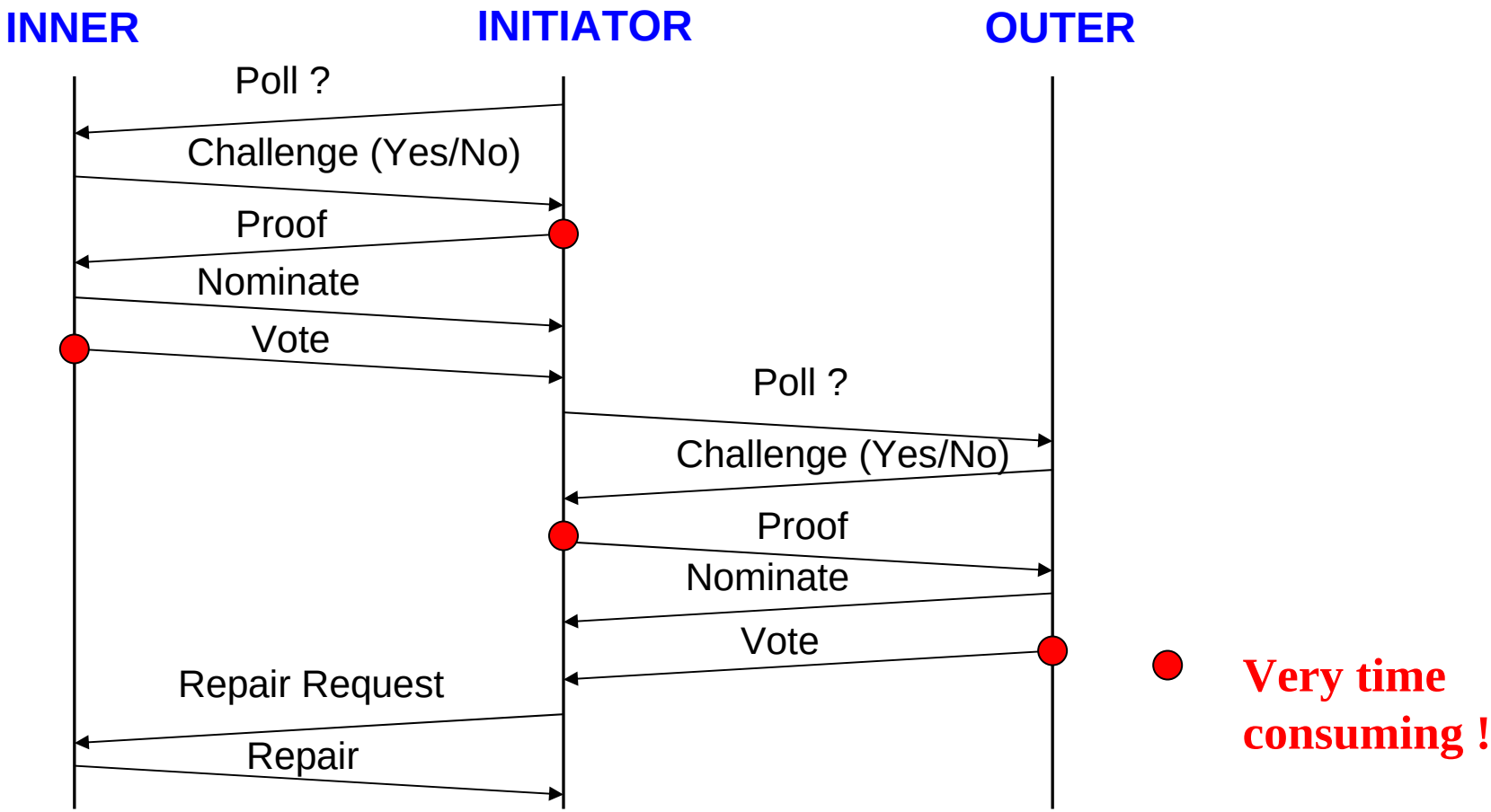
1. Invalid Vote
2. Valid Vote
   - Agreeing Vote
   - Disagreeing Vote

Protocol Description (7)



A peer supplies a repair only if the requester had previously proved with an agreeing vote that it once had the same content.

Protocol Description (8)

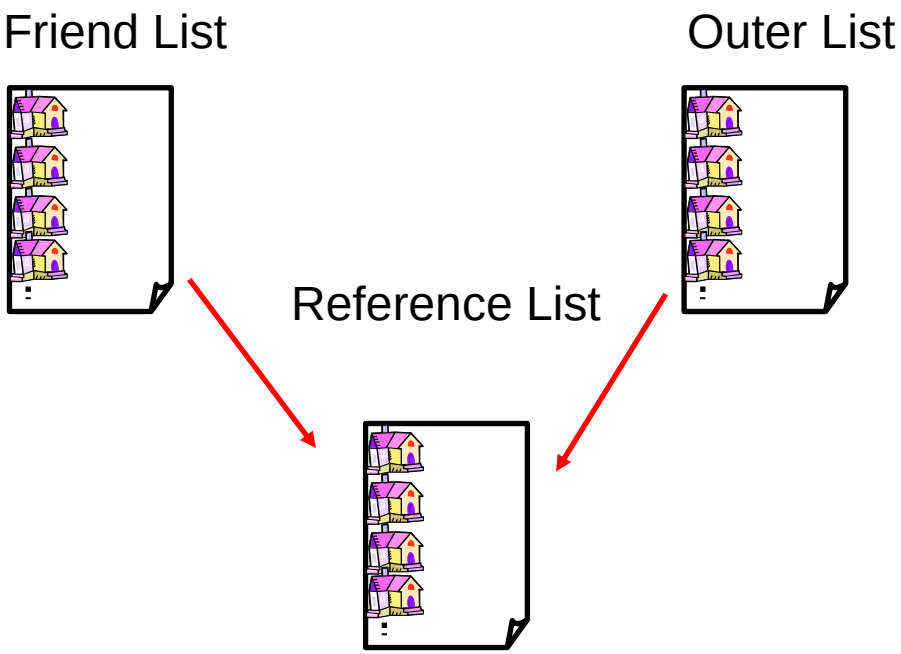


Protocol Analysis

- Reference List Churning
- Effort Sizing
- Rate Limiting
- Timeliness Of Effort
- Obfuscation of Protocol State
- Alarm

Protocol Analysis
Reference List Churning

A peer avoids depending on a fixed set of peers for maintenance of its AU.



Protocol Analysis
Effort Sizing / Rate Limiting

Large changes to a system require large effort

- Add effort involved in messages
- Rate is limited by the smaller of the adversary´s effort and the effort of his victims.

Protocol Analysis
Timeliness Of Effort

Avoid that good reputation behavior is accumulated.

- Ensure that only proofs recent effort can affect the system.

Protocol Analysis

Obfuscation of Protocol State

Assume a powerful adversary capable of observing traffic at many points of the network.

- Encrypt all but the first protocol message exchanged using a fresh symmetric key.
- Make all peers invited to a poll, even those who decline a vote, go through the motions of the protocol.

Protocol Analysis

Alarm

Intrusion Detection

The protocol raises an alarm when a peer:

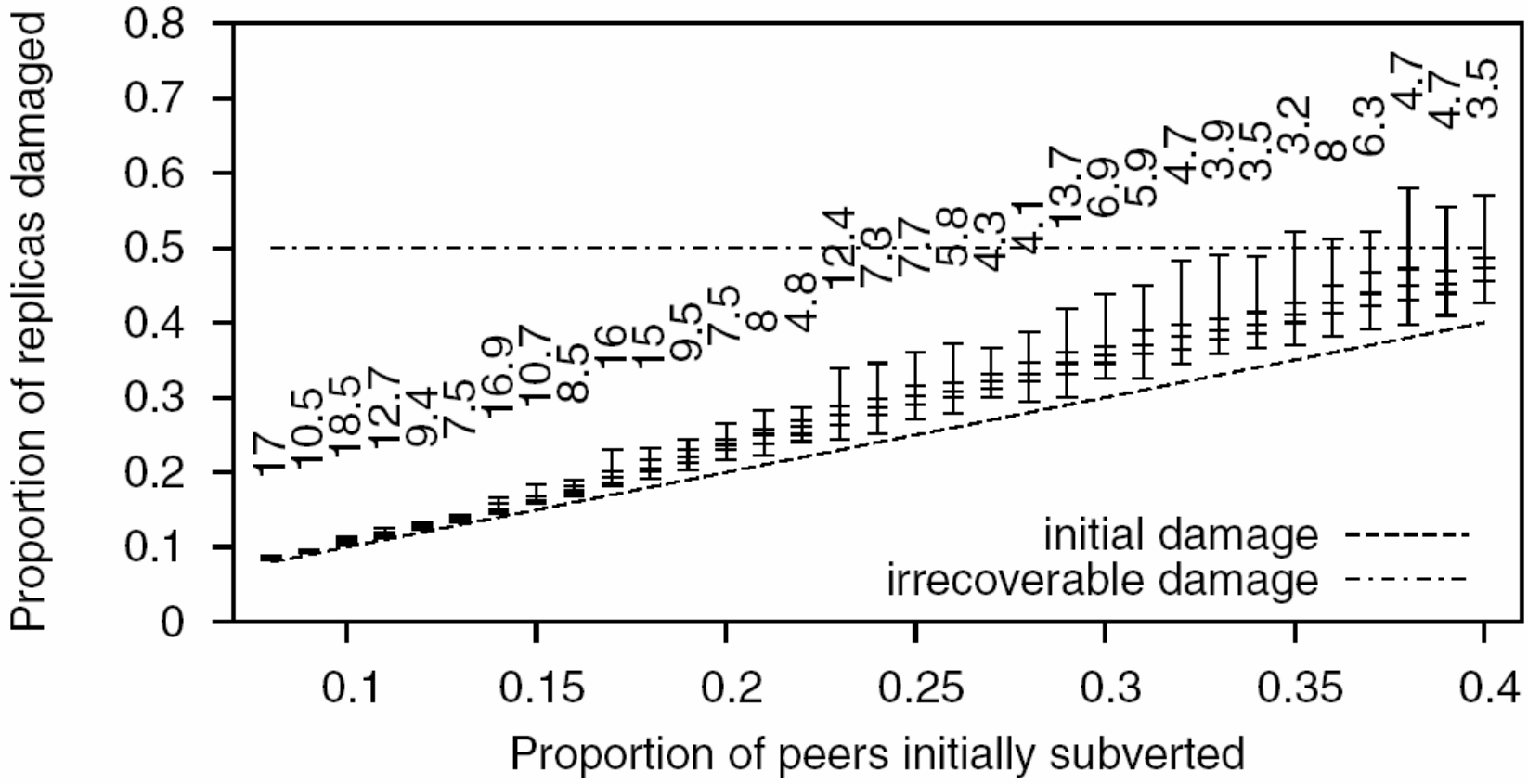
- determines that a poll in inconclusive,
- suspects local spoofing,
- has been unable to complete a poll for a long time.

Adversary

- Stealth Modification
  - The adversary's goal is to change as many replicas of the content held by loyal peers as possible without being detected.
  - Techniques:
    - Foothold in a Reference List
    - Delayed Commitment

LOCKSS: Reference List Churning, Rate-Limiting and Check consistence between repair and vote.

Results


Proportion of replicas damaged
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.1
0.15
0.2
0.25
0.3
0.35
0.4
Proportion of peers initially subverted
initial damage
irrecoverable damage
17
10.5
18.5
12.7
9.4
7.5
16.9
10.7
8.5
16
15
9.5
7.5
8
4.8
12.4
7.3
7.7
5.8
4.3
4.1
13.7
6.9
5.9
4.7
3.9
3.5
3.2
8
6.3
4.7
4.7
3.5

Conclusion

- LOCKSS can produce a peer-to-peer system with remarkable ability to resist attacks over decades.
  - Massive Replicas
  - Rate Limitation
  - Intrusion Detection (->Alarm)
  - Costly Operation

- Thank you for your attention!
- Questions?